DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	**Mandatory Vaccination Policy**	
Project Lead and Information Asset Owner/s	Project Lead	
	IAO name and asset	Jo Brown HR Director HR data
	IAO name and asset	
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acrony??ms on first use.*	**Introduction of a Mandatory Vaccination Policy in Camden**. Following a consultation with the care sector and the public, the Government has brought forward, under an amendment to the Health and Social Act 2008 (Regulated Activities) (Coronavirus) Regulations 2021 ('the Regulations'), to make vaccination a condition for any individual working in a CQC-regulated care home providing nursing or personal care in England, subject to certain exemptions. The Regulations were laid before Parliament on 22 June 2021. These were approved in the House of Lords on 20th July 2021. These Regulations provide a 16-week grace period for those covered by the legislation which started on 22nd July. Under the amendment, the Regulations apply to any professional visiting a care home, such as healthcare workers and tradespeople will also be required to show they have been vaccinated before entering the care home, unless they have a medical exemption or are out of scope e.g. people providing emergency assistance. We want to record details in the Oracle HR System of the vaccination status of frontline staff in scope of the new regulations that are required to have COVID-9 vaccination. The council is undertaking this because there is a legal requirement to do so.	

Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	16th September 2021 for first dose of the vaccination. All staff in scope are required to have both vaccination by 10th November 2021.

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	NO
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	NO
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	NO
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	NO
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of e.g. names) to become identifiable?	NO
1.6	Does the project involve multiple organisations, e.g. public sector agencies e.g. joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	YES
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	YES
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	YES
1.9	Will data be combined, compared or matched from multiple sources?	NO
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	NO
1.11	Will the personal data be processed out of the U.K? E.g. any provers have out of UK servers?	YES
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	NO
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	NO

1.14	Will personal data be processed in a way which involves tracking individuals’ online or offline location or behaviour?	NO
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	YES
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	NO

Step 2: What personal data is being used?										
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New/Changed			
							New			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	**X**	Date of Birth	**X**	Gender	**X**	National Insurance Number	NO	Financial Information about the person	**NO**
	Address	X	Email address		Telephone number		NHS No	NO	Other e.g. a reference number such as Mosaic ref	NO
	Other data *(Please state):*									
	Special Categories of Personal Data									
	Racial or ethnic origin	No	Fingerprints/ Biometrics	No	Religious or philosophical beliefs Political opinion					No
	Trade Union membership	No	Physical or mental health or condition							Yes
	Sexual life or sexual orientation	No	Housing records Social services records	No	Tax, benefit or pension records	NO	Employee/HR records			Yes
	Other data *(Please state):*	COVID-19 Vaccination status only								
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	NO								

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared?**	Data will be recorded on the employee's existing staff record on the Oracle HR system to confirm date of receiving first and second vaccine, whether they are medically exempt or have declined the vaccine for other reasons. The reasons for not having the vaccine will not be recorded. Existing data will be purged from Oracle so that we only hold data for those roles in scope of the legislation. Reporting will be done on vaccination status of staff in scope. This will be used initially to ensure compliance with the new regulations and implementation work that may include changes to the employment of staff that are not medically exempt but have chosen not to be vaccinated. Aggregated (non-individual) data will also be reported onwards to Audit (who manage the Corporate Risk Register), Directors and Camden Management Team.
3.2	**Explain in as much detail as possible why this is being done**	To comply with new regulations introduced under the Health and Social Care Act 2008 (Regulated Activities) (Amendment) (Coronavirus) Regulations 2021 ('the Regulations'). The vaccination policy is a key part of our overall COVID-secure steps to ensure a safe working environment and is in addition to other existing health and safety measures. The Health and Safety at Work etc. 1974 obliges employers to take reasonable steps to reduce risk and to require employees in scope of the legislation to protect themselves and the vulnerable people that they interact with care for.

3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes
	External organisation or partner Name	**Controller or Processor?**	**Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? Yes/No/In progress**
	Oracle	Processor	Yes contract
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		N/a
3.5	**How will the information be processed/shared? Details e.g. secure file transfer**		**Provided to manager by employee by council email and then directly entered into Oracle system by HR**

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition Art 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject. This being the Health and Social Care Act (Regulated Activities) (Amendment)	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** At 9(g) Reasons of substantial public interest (with a basis in law), Part 2 of Schedule 1 of the DPA 2018 condition is para 6 Statutory etc and government	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Not applicable

	(Coronavirus) Regulations 2021 ('the Regulations').	purposes with the underlying law being the Health and Social Care Act (Regulated Activities) (Amendment) (Coronavirus) Regulations 2021 ('the Regulations'). and (h) Health or social care (with a basis in law) with the part 1 Schedule 1 DPA18 condition being paras 1 (Employment, social security and social protection) and 2 (Health or social care purposes) with the underlying law being the Health and Social Care Act 2008 (Amendment) (Coronavirus) Regulations 2021 ('the Regulations').	
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Rights Team have advised this is appropriate**		
	N/A – There is a legal requirement to collect this information		
4.3	**How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		
	Oracle have advised they will be making functionality for vaccination requirements built-in functionality , but we do not yet have a clear timeline on when this will be delivered. In meantime positions that are in-scope of the regulations will be flagged in the Oracle HR system as requiring this 'vaccination qualification'. Ideally oracle will limit ability to input this data for employees to positions that have this flag , if this is not possible then to avoid accidental recording of vaccine data of employees out of scope or non-verified information data will be entered on to the Oracle HR system by HR staff (or line managers) once verification has been provided. Verification will be conducted as part of the implementation exercise for existing staff and ongoing as part of recruitment process or regular monitoring (e.g. should boosters become a requirement). The intention is that in the recruitment process then applicants will be asked to self- declare vaccination status when submitting application and verification will then be completed for those that are appointed into post as part of standard safe staffing checks.		

4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Processing Notice online	YES
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	YES	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject	
	NO	
4.7	**Data Retention Period - how long will the data be kept?**	
	For the duration of employment in the role that is 'in-scope' of regulations for the reason the data was collected or for a period of 6 years in accordance with our data retention policy (with the exception of those who have worked with children or vulnerable adults, which is 20 years).	
	Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Oracle	
5.2	**Where is the data stored geographically?**	
	In the existing Oracle HR Payroll system. Oracle servers are held in the Netherlands which is acceptable as the UK has an EDPB adequacy decision.	
5.3	**What roles will have access to the information?** (List individuals or staff groups)	
	HR	

	Line Managers
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Role based access control is in place
5.5	**Is there an ability to audit access to the information?**
	YES
5.6	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories data and/or criminal data?**
	n/a - covered by existing arrangements for Oracle HR system.
5.7	**Has the Information Security Manager advised on the security measures? What were their comments?**
	n/a as existing system used

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Source of risk Privacy intrusion -the data being stored relates to individual's medical record and therefore considered very personal and sensitive data. Potential impact on individuals: Individuals may consider the requirement to share this data intrusive particularly as they will have no choice and not having had the vaccination (unless they are exempt) may result in adverse actions being taken against them eg redeployment. . There may be individuals whose stated gender at work does not match their NHS gender and they may not wish their transgender status to be known. There may be individuals who are not vaccinated for health reasons and they do not wish to disclose this to their employer. All such highly intrusive cases will be dealt with by a HR Business Adviser. **Source of risk : excessive data collection** Oracle allows people out of scope of mandatory vaccination to enter their details This would result in the council collecting data excessively with privacy intrusion. They may also have concerns about potential for differential treatment/suffering detriment as a result of them sharing or refusing to share this data. **Source of risk: data is stored outside Oracle by managers and used for different purposes** Risk of breach or GDPR and corporate procedures on information	Likely Possible Likely	Moderate Moderate Moderate	12 Medium/high risk 9 Medium/high risk 12 medium/high risk

security.			
Source of risk **Inaccurate data - un-verified data is recorded for staff.** Potential impact on individuals: Inaccurate data is stored for individuals in breach of their data protection rights with additional impact on their employment. This would occur when individuals who are vaccinated falsely claim they are to avoid adverse consequences. Risk of breach or GDPR and corporate procedures on information security and non-compliance with vaccine regulations	Likely	Major	16 High risk

Step 7: Identify Measures to reduce risk

Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.*

Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by IRT/DPO*

The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.

Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Privacy intrusion	The collection of data is mandatory as the law requires it. The council is not going further than the law requires. The council must meet its statutory duties. Policies and procedures are in place to ensure that only in scope roles will have data collected. For these in scope roles, the minimum data will be collected. Any HR actions will follow policies and procedures and be fair and transparent. Clear communications to staff on what data will be used for and why will be undertaken, acknowledging that they may find the requirement intrusive. Managers and HR staff that have access to information will be reminded of the importance of ensuring the data is managed securely at all times in line with corporate standards and never stored on an unsecure shared drive/area. It is accepted that this is inherently privacy intrusive but a legal requirement and there is only limited actions the council can take to minimise this	Unchanged	12 Medium/high risk	Risk tolerated as a legal requirement
excessive data collection	Oracle will have systems to ensure that only in scope roles have data collected. If this is not possible, managers will manually collect the data from in scope groups only. To avoid any accidental recording of data for individuals outside the eligible staff group data will be input to Oracle by HR staff and Line Managers only.	Reduced	6 Unlikely and moderate: Moderate risk	yes

	Communications will tell managers which roles if any are in scope and managers will be informed if they have no roles in scope they must not require people to tell them their status. If staff volunteer this, it should not be recorded.			
data is stored outside Oracle by managers and used for different purposes	Managers will be told this is not permitted and will be dealt with as a data breach. This will be clearly communicated to all managers.	Reduced	6 Unlikely and Moderate: moderate risk	yes
un-verified data is recorded for staff.	Staff will be required to show proof of vaccination. The exact proof is to be advised, but it will be verifiable. Staff IDs are already known. Where the vaccination name does not match the employee name (for example the employee may use a pre marriage/civil partnership name at work but a different surname at home) further investigations will be required to verify status.	Reduced	Rare and Minor: Low risk	yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Medium High				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	No. Sarah Laws
DPO advice	Approved

Information Asset Owner acceptance of residual risks	Joanna Brown, Director of People and Inclusion
This DPIA will kept under review by: *(usually the author or the IAO)*	HR Strategic Lead

Version Control

Version	Reason	Date	Author(s)
0.1	**Initial Draft**	**31/08/21**	
0.2	**Additions to incomplete areas**	**05/08/221**	
0.3	**Review by IRO**	**5/8/2021**	**Sarah Laws**

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Willful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

	Score:		PROBABILITY				
			Rare	Unlikely	Possible	Likely	Almost Certain
IMPACT		Catastrophic	5	10	15	20	25
		Major	4	8	12	16	20
		Moderate	3	6	9	12	15
		Minor	2	4	6	8	10
		Negligible	1	2	3	4	5

Table 4: is the risk level acceptable?

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) This will be a link to Camden's Data Charter but this does not exist yet

1. *Effects on Residents*

a) *How does use of this data benefit our residents? (Is there evidence of this approach being likely to meet a public need?)*

●

b) *What would be the harm in not processing this data?*

●

2. *Data Bias*

a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?*

●

b) *Once errors and biases have been identified in data collections, how will they be taken into account for any future policy or service which uses this work as an evidence base?*

●

c) *Who could be negatively affected by processing this data?* (How can you show there is a **fair balance** between the **rights of individuals** and the **interests of the community**?

●

3. *Limitations of Data*

a) *How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?*

●

b) *How are you ensuring the data used is reliable? (**Data quality**)*

i) *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

-

ii) *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**) (Are all metadata and field names clearly understood)*

-

d) *How could the objectives of this project be completed without processing the data?*

-